APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/619,726	07/15/2003	Steven J. Smith	MNDSH-01004US0	7044

23910   7590   10/28/2008
FLIESLER MEYER LLP
650 CALIFORNIA STREET
14TH FLOOR
SAN FRANCISCO, CA 94108

EXAMINER
JEAN GILLES, JUDE

ART UNIT	PAPER NUMBER
2443	

MAIL DATE	DELIVERY MODE
10/28/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
	10/619,726	SMITH ET AL.
Office Action Summary	Examiner	Art Unit
	JUDE J. JEAN GILLES	2443

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>23 July 2008</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-8,10-19,21-29,31-38,40-44,46-60 and 66-72</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-8,10-19,21-29,31-38,40-44,46-60 and 66-72</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>15 July 2003</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____.

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date <u>07/23/2008</u>.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____

5)☐ Notice of Informal Patent Application

6)☐ Other: _____

U.S. Patent and Trademark Office

PTOL-326 (Rev. 08-06)   **Office Action Summary**   Part of Paper No./Mail Date 20081023

DETAILED ACTION

This Office Action is in Reply to communication filed on 07/23/2008.

Information Disclosure Statement

1.   The references listed on the Information Disclosure Statement submitted on

07/23/2008, have been considered by the examiner (see attached PTO-1449A).

Response to Amendment

2.   In this amendment, claims 1, 10-13, 21, 31-32, 40, 46, 49, 50, 60 and 68 are

amended. Claims 9, 30 and 45 are cancelled; and new Claims 71-72 have been added.

Therefore claims 1-8, 10-19, 21-29, 31-38, 40-44, 46-60 and 66-72 are pending for

reconsideration in this reply. Claims 1-8, 10-19, 21-29, 31-38, 40-44, 46-60 and 66-72

represent "YSTEMS AND METHODS FOR AUTOMATICALLY UPDATING

ELECTRONIC MAIL ACCESS LISTS".

Response to Arguments

3.   Applicant's arguments with respect to amended independent claim 1 have been

carefully considered, but are not deemed fully persuasive. Applicant's arguments are

deemed moot in view of a new ground of rejection as explained here below,

necessitated by applicants' amendment. Applicants' amendments to the independent

claims are not made in such a way to perhaps place them in condition for allowance.

The dependent claims stand rejected as articulated in the Previous Office Action and all

objections not addressed in Applicant's response are herein reiterated.

Applicants' main points of contention, that is "the recipient's access list can be updated

during a standard web browser session. This point is addressed in the rejection of

claim 1 below.

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

5.   Claims 1-8, 10-19, 21-29, 31-38, 40-44, 46-60 and 66-72 are rejected under 35

U.S.C. 103(a) as being unpatentable over Brown et al (hereinafter Brown) U.S. Pub.

20040034694 A1, in view of Gropper, U.S. Pub. No. 20020049610 A1.

Regarding claim 1 Brown teaches a computer implemented method for modifying a

list of permitted senders used by electronic mail (email) access control devices (figs. 8-

10), said method comprising:

under control of a sender:

accepting a recipient identifier (0021, see pass-code);

providing sender information along with a petition provider identifier to a recipient, the

recipient having an access list of permitted senders associated therewith (0021, 0062);

under control of the recipient:

providing the sender information to a petition provider identified by the petition

provider identifier(0062-0064);

accepting an access list petition request (petition) from the petition provider, said

petition being stored in a computer readable storage medium (0062-0064);

determining whether the petition is acceptable based on at least one off 1) a sender

identity verification method; 2) user input; and 3) third party information (figs 8-10; 0062-

0065); and

modifying said access list of permitted senders of the recipient such that the sender is

added to said access list if the petition is determined to be acceptable (0062, and 0064);

and

wherein the access list is used to determine whether email from the sender is permitted

to reach the recipient (figs 8-10; 0062-0065). Brown does not teach the specific step of

"*accepting, by way of a web browser on the recipient, an access list petition request

(petition) from the petition provider, said petition being stored in a computer readable

storage medium, wherein the petition is transmitted via hypertext transfer protocol

(HTTP) as part of an interaction with a web page*". Nonetheless, this feature is well-

known in the art and would have been an obvious modification to the system of Brown,

as evidenced by Gropper.

In the same field pf endeavor, Gropper discloses that a system used a web page to update an address book following a request from the sender and the update is transmitted via the internet using an updated request from or web page. Gropper teaches "The server program validates that the recipient is the intended recipient and then displays an update request form (a web page) via which the recipient can confirm, edit or add to the presented ("existing") content (i.e. the information which the sender has about the addressee in the sender's address book)...The server system then stores the recipient's response (i.e. updated content) until the next time the client program communicates with the server program" (see Gropper, par. 0084). In order to facilitate updating of the user's address book without necessarily sending an email reply, using the web setting (web page) for direct reply via HTTP makes sense.

Accordingly, it would have been obvious for an ordinary skill in the art at the time the invention was made to incorporate the teaching of Gropper within the structure of Brown, making it easy and desirable for users to promote use of the system to their contacts, thereby avoiding the labor and errors associated with manual data entry and maintenance of contact information into a digital address book (see Gropper, par. (0003-0004). By this rationale, claim 1 is rejected.

Regarding claims 1-8, 10-19, 21-29, 31-38, 40-44, 46-60 and 66-72, the combination Brown- Gropper teaches:

2. The method of claim 1 wherein:

the sender information includes at least one of: 1) a sender identification method; and 2)

the recipient identifier (Brown, 0024, 0051, and 0061).

3. The method of claim 1, further comprising:

providing confirmation of the determination to the sender (Gropper, 0084, 0216).

4. The method of claim 1 wherein:

the step of accepting the recipient identifier is a result of a Web-based interaction

between the recipient and the sender (see Gropper, 0020, 0084). .

5. The method of claim 1 wherein:

the recipient identifier is an email address (Brown, 0024, 0051, and 0061).

6. The method of claim 1 wherein:

the identity verification method is one of: 1) an email header "From" address; 2) a

password; 3) an Internet Protocol (IP) address; and 4) a digital signature (Brown; fig. 6-

7).

7. The method of claim 1 wherein:

the step of determining whether a petition is acceptable utilizes at least one rule,

wherein the at least one rule is evaluated against the petition (Brown; 0057).

8. The method of claim 1, further comprising:

prompting a user for a decision regarding whether or not to accept the petition (Brown; fig. 10).

10. The method of claim 9 wherein:

the sender information is provided to the petition provider via a Hypertext Transfer Protocol (HTTP) redirect sent to the Web browser (Brown; 0032).

11. The method of claim 1 wherein:

the petition is provided to a petition processor via a Hypertext Transfer Protocol (HTTP) redirect message sent to the Web browser (Brown; fig. 1); and

wherein the petition processor makes said determination (Brown; fig. 1).

12. The method of claim 1 wherein:

the Web browser identifies the petition based on a Multipurpose Internet Mail Extension (MIME) type (Brown; 0043).

13. The method of claim 1 wherein:

the petition provider identifier and the sender information are combined to form a Uniform Resource Locator (URL) that the Web browser uses to access the petition provider (Brown; fig. 1).

14. The method of claim 1, further comprising:

providing the petition to a petition processor (Brown; fig. 1).

15. The method of claim 14 wherein:

the petition processor requires authorization credentials (Brown; see passcode, 0064).

16. The method of claim 1 wherein:

the sender identity verification method is used by an email provider to verify that an email message is from the sender (Brown; 0064).

17. The method of claim 1 wherein:

the petition provider generates the petition based on one or more rules (Brown; 0057).

18. The method of claim 17 wherein:

a rule determines at least one of: 1) whether to generate the petition; 2) a format of the petition; 3) an identity of a petition processor; and 4) a recipient email address (Brown; 0057, 0062-0064).

19. The method of claim 17 wherein:

a rule is triggered based on the recipient identifier 0057, 0062-0064).

21. A computer implemented method for modifying a list of permitted senders used by electronic mail (email) access control devices (Brown; figs 8-10), said method comprising:

under control of a sender:

accepting a recipient identifier (Brown; 0021);

generating an access list petition request (Brown; petition) wherein said generation is

based on the evaluation of at least one rule that determines the format of the petition

based on the recipient identifier, said petition being stored in a computer readable

medium (Brown; figs 8-10; 0062-0064);

providing the petition to a recipient, the recipient having an access list of

permitted senders associated therewith;

under control of the recipient:

accepting the petition by way of a web browser on the recipient, wherein the petition is

transmitted as part of an interaction with a web page and prior to transmission of email

messages between the sender and the recipient (Gropper; 0084; 0020);

determining whether the petition is acceptable based on at least one of: 1) a sender

identity verification method; 2) user input; and 3) third party information (Brown; 0057;

0062-0064); and

modifying said access list of permitted senders of the recipient such that the sender is

added to said access list if the petition is determined to be acceptable (0062, and 0064);

wherein the access list is used to determine whether email from the sender is permitted

to reach the recipient (Brown; figs 8-10; 0062-0064).

22. The method of claim 21, further comprising:

providing the recipient identifier to a petition provider; and

accepting a petition from the petition provider (Brown, 0024, 0051, and 0061).

23. The method of claim 21 wherein:

the sender information includes at least one of: 1) a sender identification method; and 2)

the recipient identifier (Brown, 0024, 0051, and 0061).

24. The method of claim 22 wherein:

the petition provider and the sender are part of the same system (Brown; fig. 1).

25. The method of claim 21 wherein:

the step of accepting the recipient identifier is a result of a Web-based interaction

between the recipient and the sender (Brown; fig. 1).

26. The method of claim 21 wherein:

the recipient identifier is an email address (Brown; figs 6-7).

27. The method of claim 21 wherein:

the identity verification method is one of: 1) an email header "From" address; 2) a

password; 3) an Internet Protocol (IP) address; and 4) a digital signature (Brown; figs 6-

7).

28. The method of claim 21 wherein:

the step of determining whether a petition is acceptable utilizes at least one rule,
wherein the at least one rule is evaluated against the petition (Brown; 0057).

29. The method of claim 21, further comprising:

prompting a user for a decision regarding whether or not to accept the petition (Brown;
fig. 10).

31. The method of claim 30 wherein:

the petition is provided to a petition processor via a Hypertext Transfer Protocol (HTTP)
redirect sent to the Web browser; and wherein the petition processor makes said
determination (Brown; fig 1).

32. The method of claim 30 wherein:

the Web browser identifies the petition based on a Multipurpose Internet Mail Extension
(MIME) type (Brown; 0043).

33. The method of claim 21, further comprising:
providing the petition to a petition processor (Brown; fig. 2).

34. The method of claim 33 wherein:

the petition processor requires authorization credentials (Brown; passcode).

35. The method of claim 21 wherein:

the sender identity verification method is used by a petition processor to verify that an

email message is from the sender (Brown; 0061-0062).

36. The method of claim 22 wherein:

the petition provider generates the petition based on one or more rules (Brown; 0057).

37. The method of claim 36 wherein:

a rule determines at least one of: 1) whether to generate the petition; 2) a format of the

petition; 3) an identity of a petition processor; 4) a recipient email address (Brown; 0057;

0062-0064).

38. The method of claim 36 wherein:

a rule is triggered based on the recipient identifier (Brown; 0057).

40. A computer implemented method for modifying a list of permitted senders used by

electronic mail (email) access control devices (figs 8-10), said method comprising:

providing a recipient email address to the sender;

receiving a petition to the recipient, receiving a petition to the recipient wherein the

petition is transmitted as part of a web browser-based interaction with a web page, prior

to transmission of emails between the sender and the recipient and Gropper, 0020,

0084) wherein the petition includes a sender identity

verification method (Brown; 0021-0024);

determining whether the petition is acceptable based on authorization credentials and at least one of: 1) the sender identity verification method; 2) user input; and 3) third party information (Brown; 0062-0065);

modifying an email access list of permitted senders by adding the sender to said email access list if the petition and the authorization credentials are acceptable (Brown; 0021-0024; (0062, and 0064);

wherein the email access list is used to determine whether or not email from the sender is permitted to reach the recipient (Brown; 0021-0024; 0062-0065).

41. The method of claim 40, further comprising:

providing confirmation of the determination to the sender(Gropper, 0084, 0216).

42. The method of claim 40 wherein:

the step of providing the recipient email address to the sender is a result of a Web-based interaction between the recipient and the sender (Brown; fig. 1).

43. The method of claim 40 wherein:

the sender identity verification method is used by the recipient to verify that an email message is from the sender (Brown; 0021-0024).

44. The method of claim 40 wherein:

the identity verification method is one of: 1) an email header "From" address; 2) a password; 3) an Internet Protocol (IP) address; and 4) a digital signature (Brown; 0057).

46. The method of claim 40 wherein:

the Web browser identifies the petition based on a Multipurpose Internet Mail Extension

(MIME) type (Brown; 0043).

47. The method of claim 40 wherein:

the step of determining whether a petition is acceptable utilizes at least one rule,

wherein the at least one rule is evaluated against the petition (Brown; 0057).

48. The method of claim 40, further comprising:

prompting a user for a decision regarding whether or not to accept the petition (Brown;

fig. 10; 0062).

49. A system comprising:

a means for providing a recipient email address to the sender;

a means for receiving a petition to the recipient, receiving a petition to the recipient

wherein the petition is transmitted as part of a web browser-based interaction with a

web page, prior to transmission of emails between the sender and the recipient and

Gropper, 0020, 0084) wherein the petition includes a sender identity

verification method (Brown; 0021-0024);

a means for determining whether the petition is acceptable based on authorization

credentials and at least one of: 1) the sender identity verification method; 2) user input;

and 3)

third party information; a means for modifying an email access list of permitted senders

by adding the sender to said email access list if the petition and the authorization

credentials are acceptable (Brown; 0021-0024);

wherein the email access list is used to determine whether or not email from the sender

is permitted to reach the recipient (Brown; 0062-0065).

50. A system for modifying a list of permitted senders used by

electronic mail (email) access control devices (Brown; figs 8-10), said method

comprising :

a sender component that accepts a recipient identifier and generates sender

information, wherein the sender information is used to generate a petition(Brown; 0021-

0024);

a petition provider component that generates a petition based on the sender

information and at least one rule, said petition being stored in a computer readable

medium (Brown; 0021-0024); and

a recipient that receives the petition from the petition provider component by way of a

web browser on the recipient, determines whether the petition is acceptable and

modifies the email access list of permitted senders, wherein the petition is

transmitted as part of a web browser-based interaction with a web page, prior to

transmission of emails between the sender and the recipient (Gropper, abstract; 0084)

and;

wherein the petition includes a sender identity verification method which change is used to verify the identity of the sender (Brown; 0062-0065).

51. The system of claim 50, further comprising:

a web browser operable to accept the sender information from the sender component and provide the sender information to the petition provider component (Brown; fig. 1).

52. The system of claim 50, further comprising:

a petition processor component operable to accept the petition and determine whether the petition is acceptable based on at least one of: 1) the sender identity verification method; 2) user

input; and 3) third party information; and

wherein if the petition is acceptable, the sender component is permitted to send email to a recipient associated with the recipient identifier (Brown; fig. 10).

53. The system of claim 52, further comprising:

a web browser operable to accept the petition from the petition provider component and to provide the petition to the petition processor (Brown; fig. 1).

54. The system of claim 52 wherein:

the petition processor component provides a confirmation to the sender (Gropper, 0084, 0216).

55. The system of claim 52 wherein:

the browser identifies the petition based on a Multipurpose Internet Mail Extension
(MIME) type (Brown; 0043).

56. The system of claim 50 wherein:

the sender identification verification method is one of: 1) an email header "From"
address; 2) a password; 3) an Internet Protocol (IP) address; and 4) a digital signature
(Brown; fig. 5-6).

57. The system of claim 52 wherein:

the petition processor determines whether or not to accept a petition and add the
sender to an email access list for a recipient (Brown; fig. 10).

58. The method of claim 50 wherein:

the at least one rule determines at least one of: 1) whether to generate the petition; 2) a
format of the petition; and 3) an identity of a petition processor (Brown; fig. 3).

59. The method of claim 50 wherein:

the at least one rule is triggered based on the recipient identifier (Brown; fig. 5-6)).

60. A machine readable medium having instructions stored thereon that when executed
by a processor cause a system to:
accept a recipient identifier (Brown; 0021-0024);
provide a petition to a recipient by way of a web browser on the recipient, said petition
being transmitted to the recipient as part of a web browser-based interaction with a web

page (Gropper, 0084), wherein the recipient corresponds to the recipient

identifier and wherein the petition is based on the evaluation of at least one rule, said

recipient having an access list of permitted senders associated therewith (Brown; 0062-

0065; see abstract);

determine whether the petition is acceptable based on at least one of: 1) a sender

identity verification method; 2) user input; and 3) third party information (Brown; 0062-

0065); and

modifying said access list of permitted senders of the recipient such that a sender

associated with said petition is added to the access list if the petition is determined to be

acceptable (0062, and 0064);

wherein the petition is created as a result of accepting the recipient identifier; and

wherein if the petition is acceptable, the sender is permitted by the access list to

send email to the recipient (Brown; 0062-0065).

66. The method of claim 1 wherein modifying the access list adds the sender to at

least one of: a white list of senders permitted to send email to the recipient and a black

list of senders prohibited from sending email to the recipient (Gropper, 0020, 0084).

67. The method of claim 1, further comprising:

communicating, from the recipient to the sender, a confirmation of the outcome of the

petition that specifies whether the sender was added to the access list of the

recipient(Gropper, 0084, 0216).

68. A computer readable storage medium having instructions stored thereon, which

instructions when executed by one or more processors, cause a system to:

under control of a sender:

accept a recipient identifier (Brown; 0021);

provide sender information along with a petition provider identifier to a recipient,

the recipient having an access list of permitted senders associated therewith (Brown;

0021-0024);

under control of the recipient:

provide the sender information to a petition provider identified by the petition

provider identifier;

accept, by way of a web browser on the recipient, an access list petition request

(petition) from the petition provider, said petition being stored in a computer readable

storage medium, wherein the petition is transmitted via hypertext transfer protocol

(HTTP) as part of an interaction with a web page (see Gropper, par. 0084);

determine whether the petition is acceptable based on at least one of: 1) a

sender identity verification method; 2) user input; and 3) third party information; and

modify said access list of permitted senders of the recipient such that the sender

is added to said access list if the petition is determined to be acceptable (Brown; 0021-

0024; 0062, and 0064); and

wherein the access list is used to determine whether email from the sender is
permitted to reach the recipient (Brown; fig. Fig. 8-10; 0062-0065).

69. The computer readable storage medium of claim 68 wherein modifying the access
list adds the sender to at least one of: a white list of senders permitted to send email to
the recipient and a black list of senders prohibited from sending email to the recipient
(Gropper, 0084, 0020).

70. The computer readable storage medium of claim 68, further comprising
instructions that cause the system to:

communicate, from the recipient to the sender, a confirmation of the outcome of the

petition that specifies whether the sender was added to the access list of the recipient
(Brown; 0062; fig. 10; Gropper, 0084, 0216).

71. The method of claim 1, wherein said method is initiated by providing the
recipient identifier to the sender as a part of a web browser-based interaction between
the recipient and the sender (Gropper, 0084, 0216).

72. The method of claim 1, wherein the recipient includes a petition processor
integrated into said web browser, the petition processor determining whether the
petition received from the petition provider is acceptable (Gropper, 0084, 0216; Brown;
fig. 1).

Conclusion

6.   Applicant's amendment necessitated the new ground(s) of rejection presented in

this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37

CFR 1.136(a).

        A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from examiner

should be directed to Jude Jean-Gilles whose telephone number is (571) 272-3914.

The examiner can normally be reached on Monday-Thursday and every other Friday

from 8:00 AM to 5:30 PM.

        If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Tonia Dollinger, can be reached on (571) 272-4170. The fax phone number

for the organization where this application or proceeding is assigned is (571) 273-3301.

Any inquiry of a general nature or relating to the status of this application or

proceeding should be directed to the receptionist whose telephone number is (571) 272-

0800.

/Jude J Jean-Gilles/

Primary Examiner, Art Unit 2443

October 22, 2008